増えるアカウントや権限の
管理業務をどう考えればよいのか？

ID管理業務の基礎と、各システムとの連携

Keyspider Japan LLC

自己紹介　潮村　剛

- 1990年代半ば、食品メーカーからソフトウェア業へ。
  国内の主要通信キャリア向けを中心に、
  セキュリティシステム案件を100件以上手がける。
- 2008年かもめエンジニアリング設立。
  統合認証基盤やビッグデータ処理を開発・提供
  2017年からSSOソリューションを展開し、
  SSOやID管理の課題を解決する専門チーム。
- 企業のID管理の課題解決をしたいと願い、
  Keyspider Japanを2019年に仲間と設立、
  Keyspiderマネージドサービスを展開中。
- オライリー・ジャパン刊行の
  『RADIUS – ユーザ認証セキュリティプロトコル』
  『Diameter プロトコルガイド』を仲間と出版。
- 剣道四段。指導員資格あり。ただし最近はサボり中。

画像引用:
オライリー・ジャパン

本日お伝えすること

- ID管理とは
- ID管理業務の基礎
- ID管理のシステム
- 各システムとの連携
- 質疑応答

■ID管理とは

ID管理、大変じゃないですか？

- ✓ 新入社員が入社した
- ✓ ○○さんに権限付与
- ✓ 全社的な人事異動
- ✓ ○○さんの権限削除
- ✓ ○○さんが退職
- ✓ ：

<クラウド>

- Office365、G Suite などのオフィススイート
- Salesforce などのCRM
- BOX などのオンラインストレージ
- Slack、LINEWORKS、ChatWork などのビジネスチャット
- Zoom、Teams などのビデオ会議
- サイボウズ、Kintone などのグループウェアやWebデータベース
- コンカー、楽々精算、マネーフォワード などの経費精算
- ジョブカン、KING OF TIME などの勤怠管理

<社内システム>

監査法人の視点

- IT全般統制のフレームワークの一部
  - アクセス管理
    - 論理アクセス管理
      - ユーザーID
        - » 割り当て・変更・削除
        - » データアクセス、DL権限などの権限付与申請・承認
        - » パスワード管理（初期パスワード通知、初期パスワード強制変更、パスワードの複雑性、有効期間、パスワードリセット）
        - » 使用状況のモニタリング
        - » 棚卸し
      - 特権ID、埋め込みID
      - その他
    - 物理アクセス管理

監査法人の視点

1）見るべきポイントが全部
「**手続き**に落ちているかどうか」

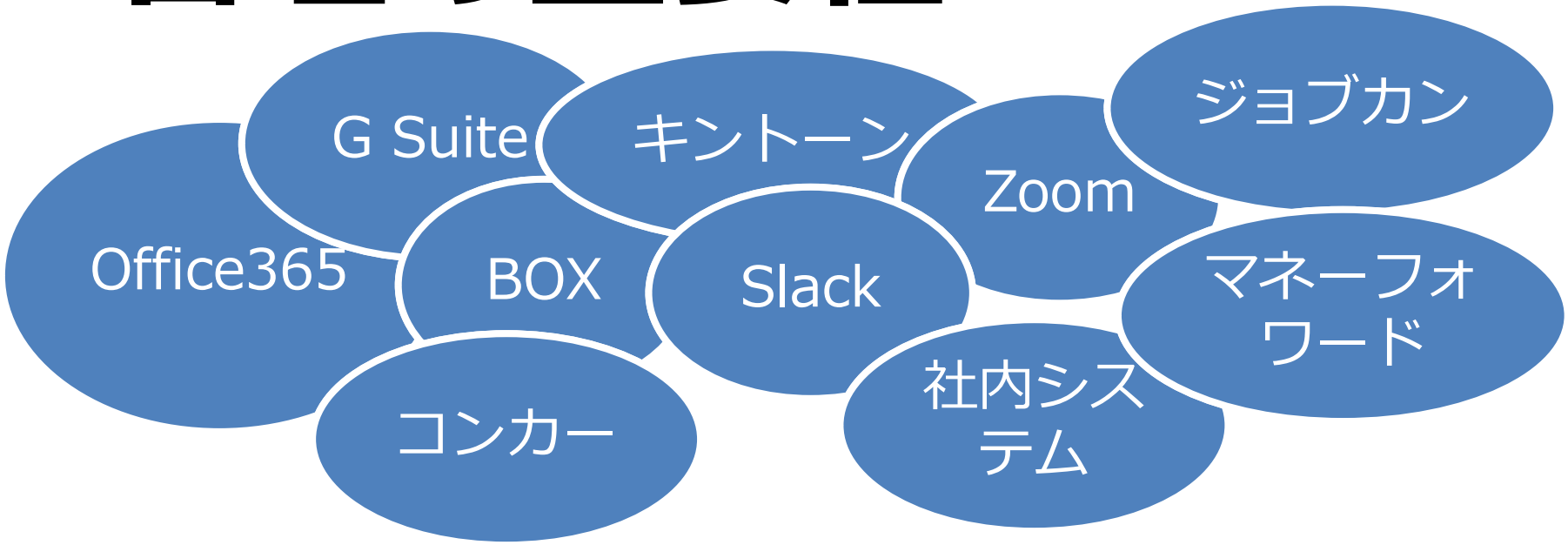
手順書 or システム

2）その手続きについて
「責任が明確になっているかどうか」

3）**その手続き通りに**
「運用されているかどうか」

手作業では難しい
システム化が必要

ID管理の重要性



アクセス（権限）制御／監査証跡

認証基盤

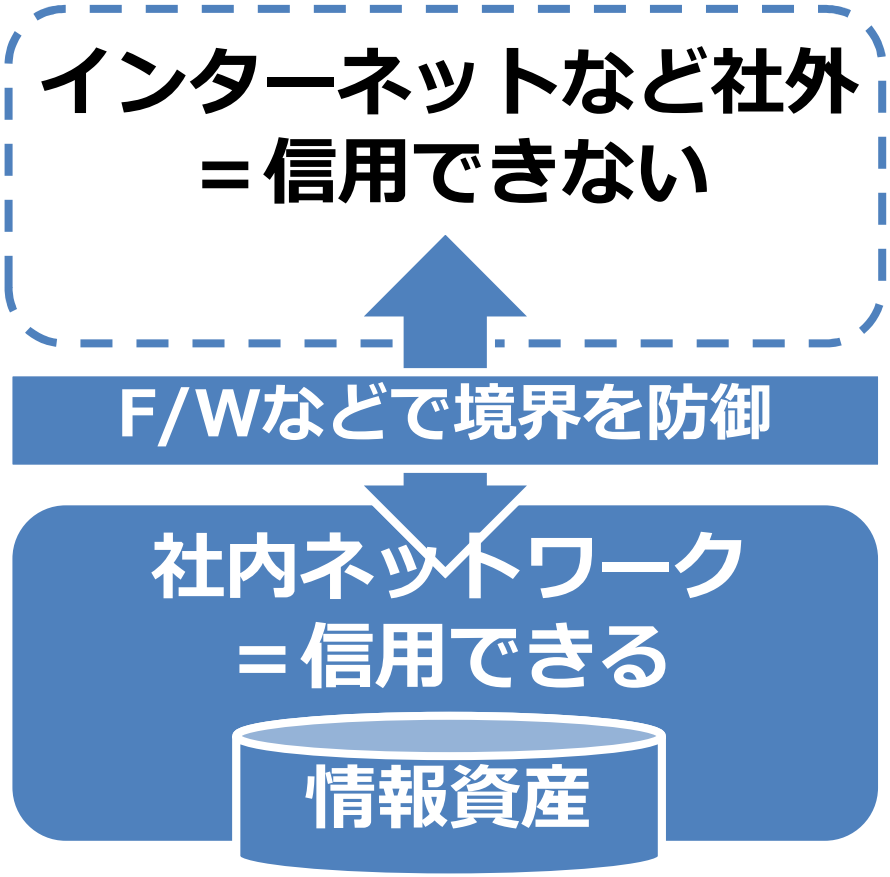
ID管理

セキュリティ対策の根幹

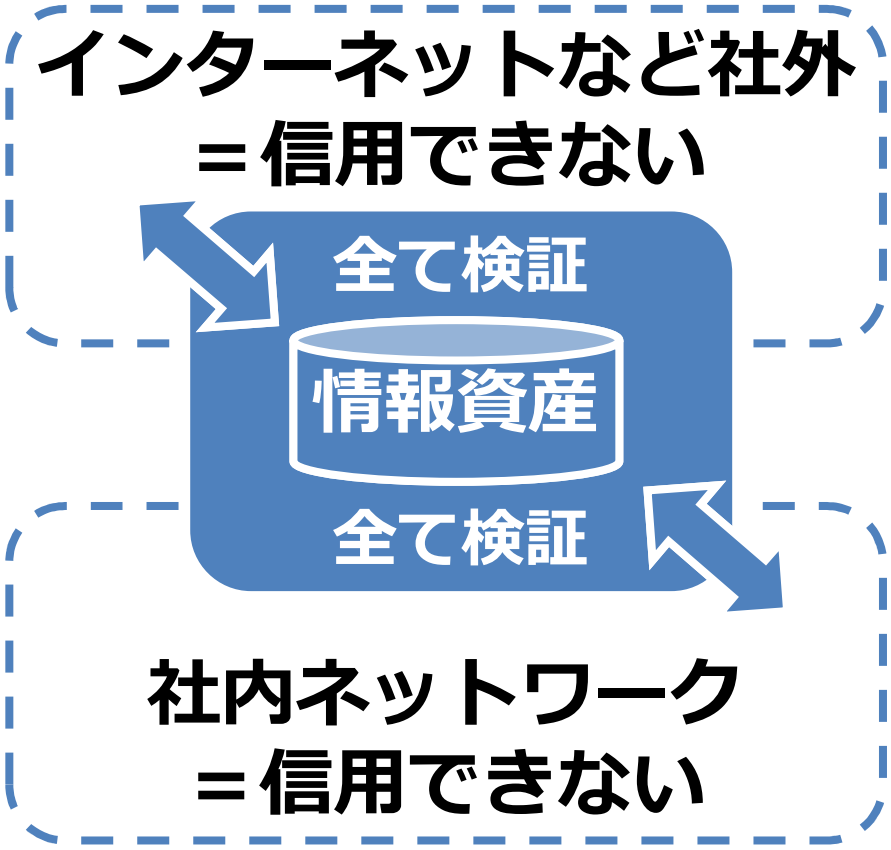
■ゼロトラスト

ゼロトラスト

境界防御モデル

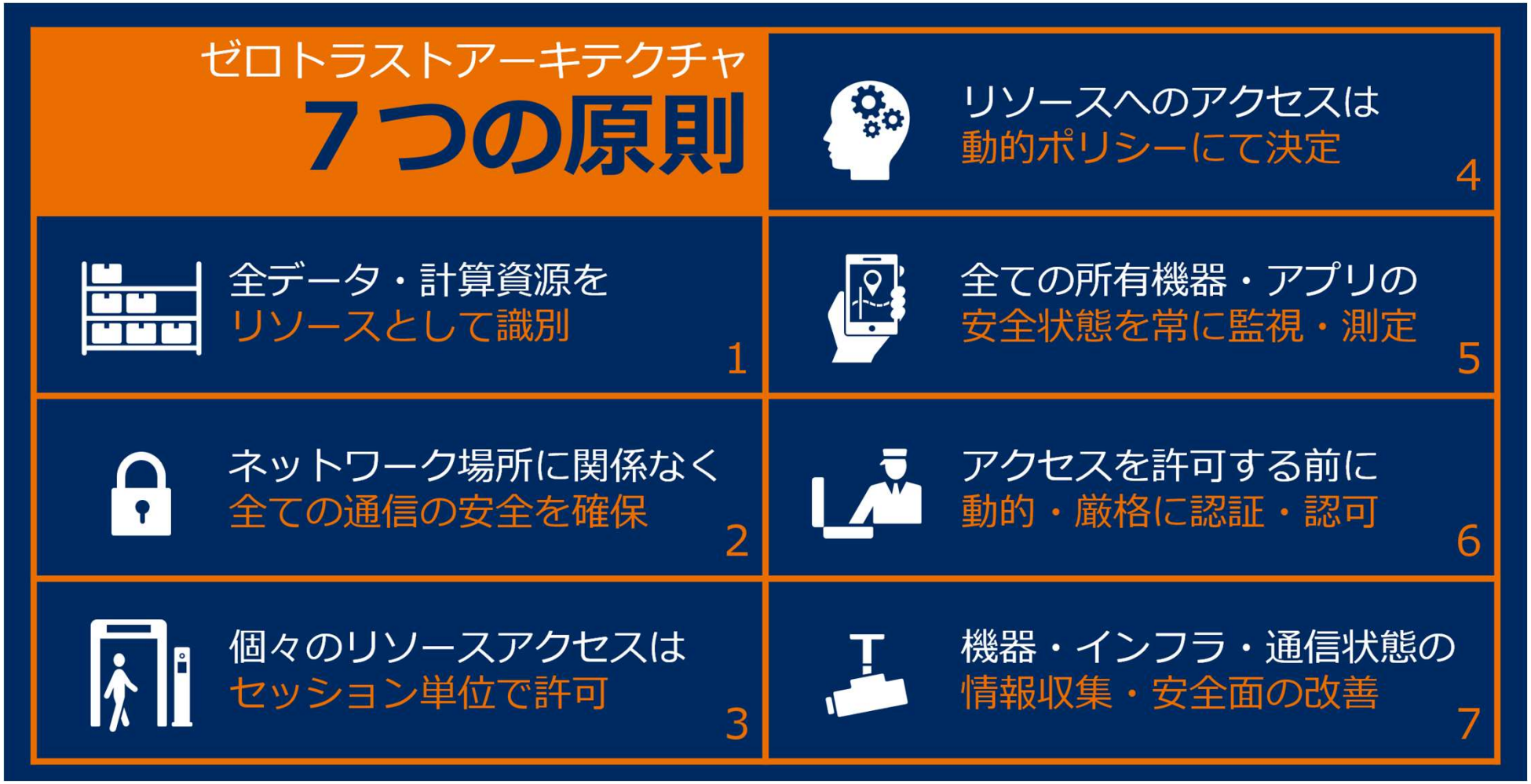


ゼロトラストモデル



ゼロトラストアーキテクチャ

■ アメリカ国立標準技術研究所（NIST）の定義する7つの原則



出所）https://jpn.nec.com/cybersecurity/blog/201016/index.html

■ID管理業務の基礎

ID管理業務の基礎

- アカウント（ユーザー、属性）、組織、グループ、権限を管理
  - 一元管理し、追加、変更、削除を行う
  - 全てのシステムに同期に同期する
- パスワード管理
  - パスワードポリシーの策定、順守
  - パスワードリセット

ID管理業務の基礎

- アカウント作成、権限付与の承認
  - 例えば取引先社員のアカウント作成時、グループ管理者権限の社員への付与時など、担当者が申請し責任者の承認を得る
- 監査
  - 不正発覚時に追跡できるように、記録（いつ、誰が、何をした）、保管
  - 異常値（パスワードリセットが多いなど）があったときのアラート
- 棚卸
  - 管理上の状態（アカウント、権限）と、実際の現場の状態との差分をチェック

権限、認可はどう整理する？

■問題
- ●システムによって、権限の考え方、体系は様々
- ●役職だけ全てに対応できるわけではない

■対応
- ●各システム側の権限設定において、組織、役職で対応可能なものはそれで対応
- ●「グループ」は各システム共通の意味合いを持たせる
- ●各システム固有の管理権限などは無理に統一しようと考えない

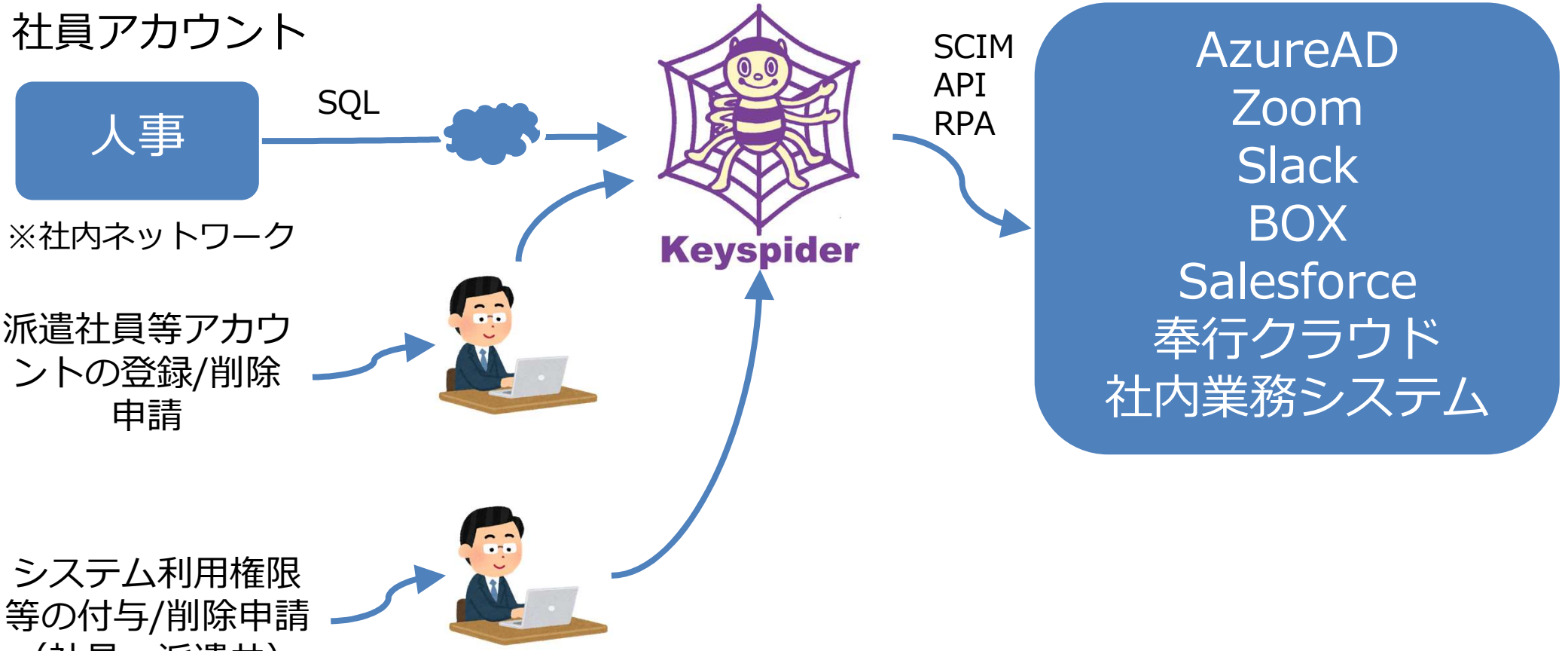
申請ってどう整理する？

＜Keyspider導入時に無償で実施させて頂いている内容＞

- 申請の種類は以下想定しています。
  - 派遣社員等のアカウント登録／削除申請
  - システム利用申請／削除申請
  - システム内部の権限付与／削除申請
- お客様に対するヒアリング（1～2時間程度を想定）を実施し、以下について整理します。
  - 申請の一覧
  - 各申請について、誰がどのように承認、設定等の作業を行うか
  - Keyspiderの設定をどうするか
- アウトプットは以下を想定しています。
  - 上記を整理した一覧（Excel）
  - Keyspiderの設定シート

  ※手順書の作成は作業に含みません

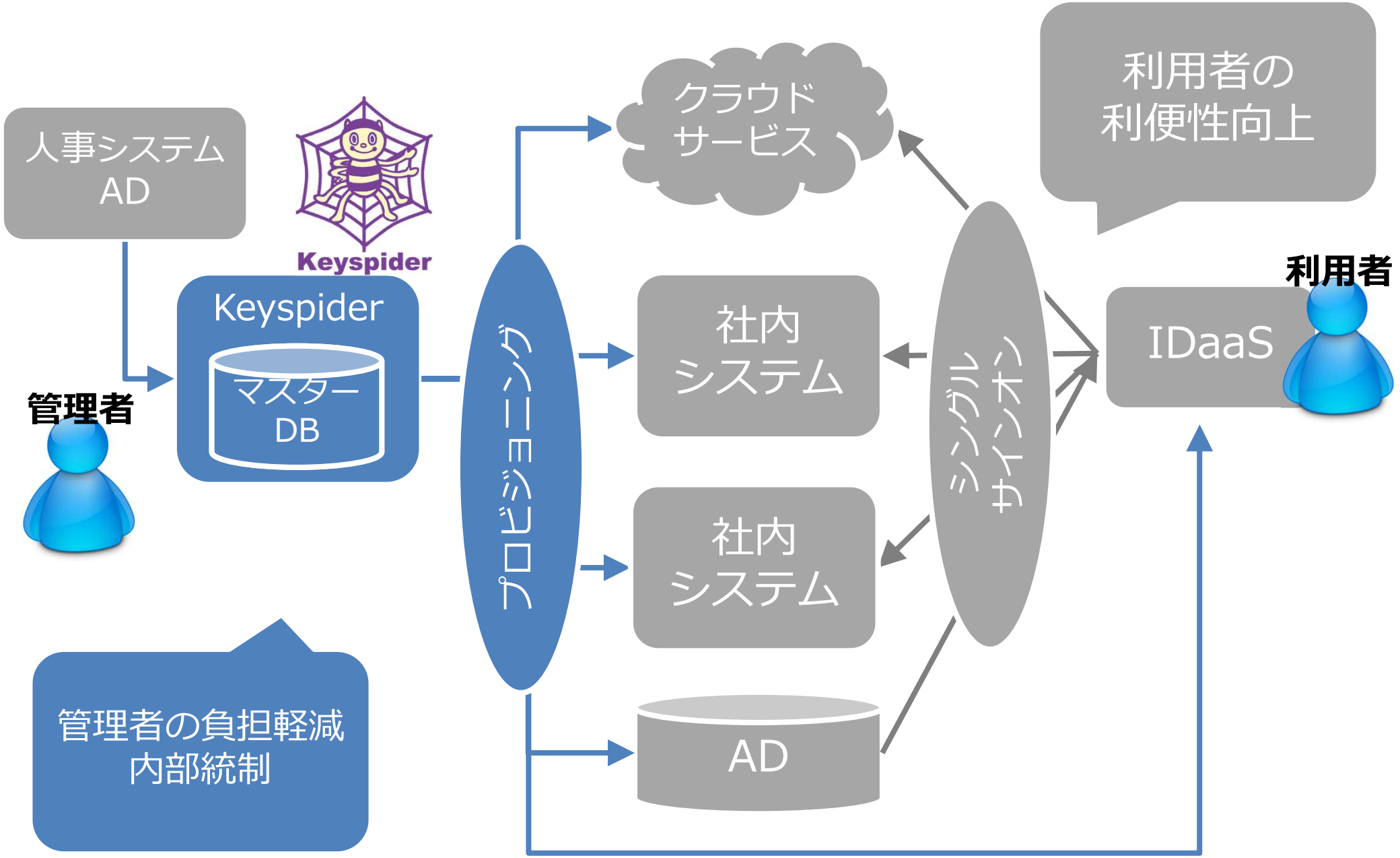
実際のシステムイメージ



役職者等権限付与できる方をKeyspider Managerの管理者として登録。
メール等で申請を受けた場合、Keyspider Managerにログインし、手動で権限を付与。
将来的にはワークフロー化を検討。

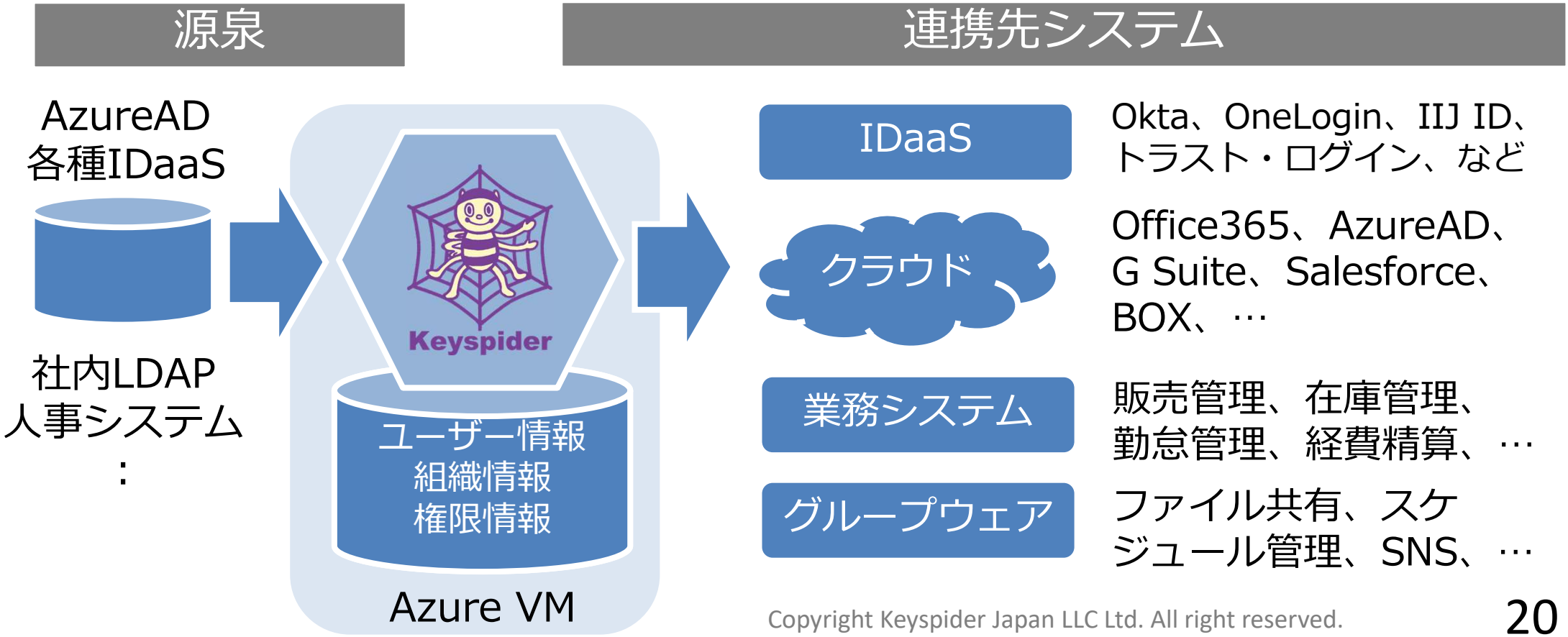
■ID管理のシステム（Keyspider）

企業の認証基盤における、Keyspiderの位置付け
～シングルサインオンを実現するにも、前提として統合ID管理が必要～



Keyspiderとは

- Keyspiderは、AzureAD、Office365、Salesforce、G Suite、BOXなどのクラウドサービスはもちろん、オンプレの社内システムとも、簡単にID連携できる、ID管理マネージドサービスです。
- 企業内のそれぞれのシステムに存在するユーザーID、パスワードや、組織、権限情報などを、一元的に管理し、企業内のすべてのシステムに同期。企業内のユーザー情報、権限情報を統合的に管理します。



なぜKeyspiderが必要なのか

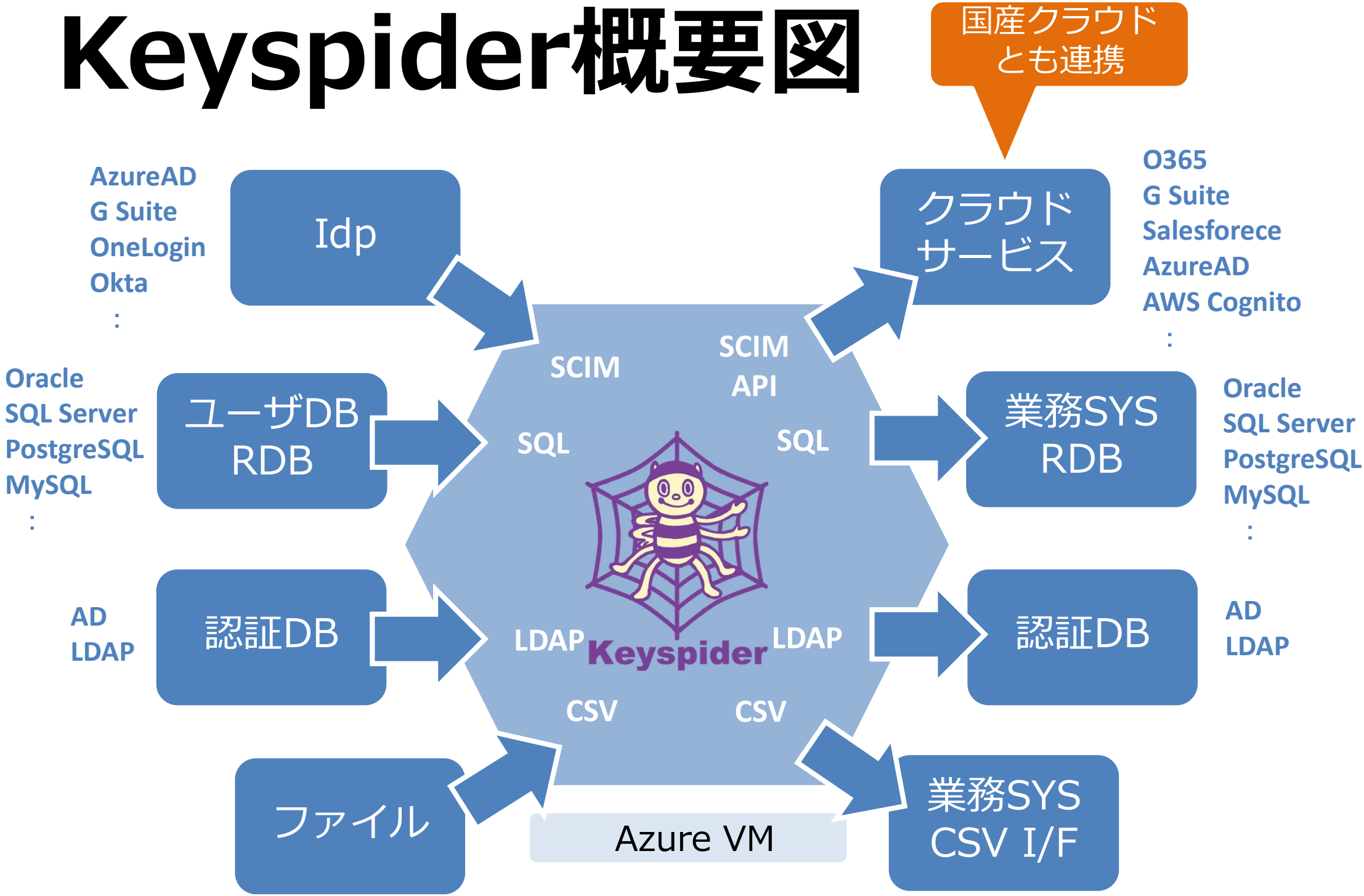
＜管理の効率化＞

- 入社時、退社時の作業のアカウント追加/削除作業の自動化
- 人事異動時の全システムの権限洗い替え作業の自動化

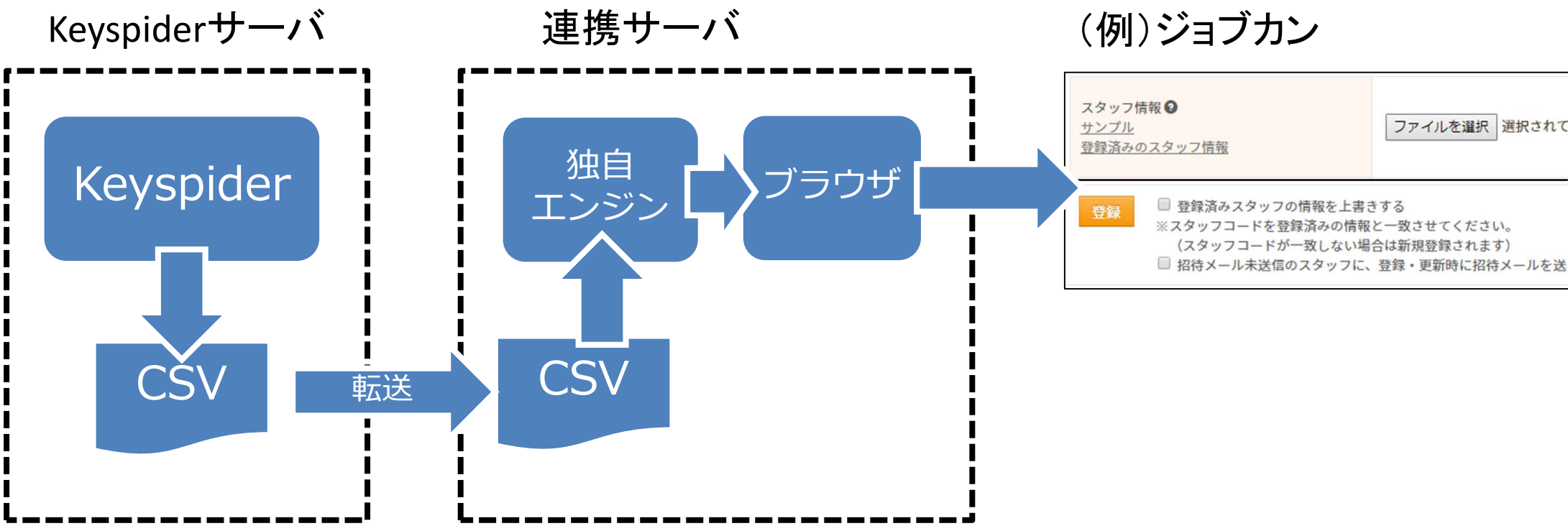
＜セキュリティ＞

- 内部統制の監査対応（退社時や異動による権限喪失時に、速やかに全システムに反映など）
- ユーザー追加やユーザーへの権限付与などについて、いつ、どのように行われたのか、監査ログの記録
- 各システムでのアクセス制御、監査ログ記録のベースとなるユーザIDの適切な管理

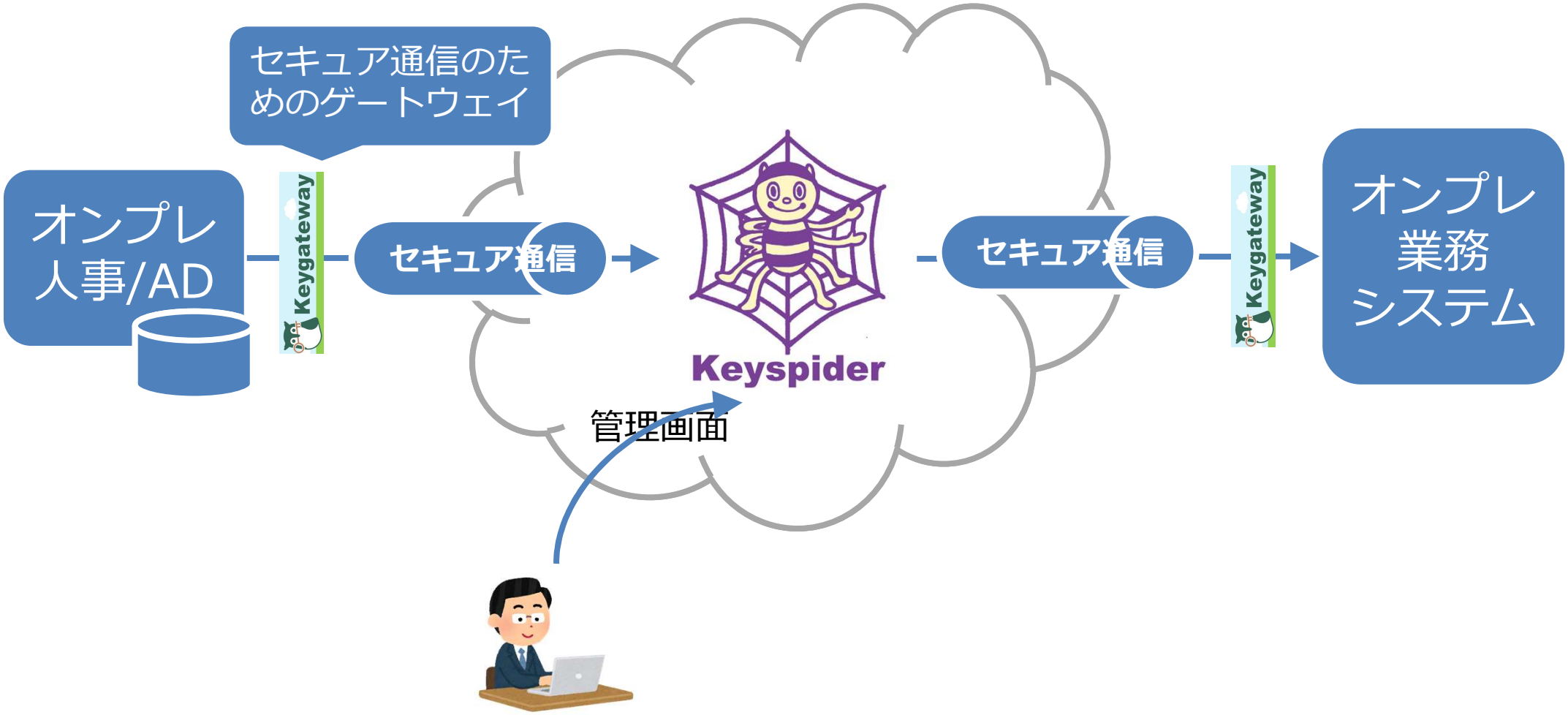
Keyspider概要図



APIが無い国産クラウドも



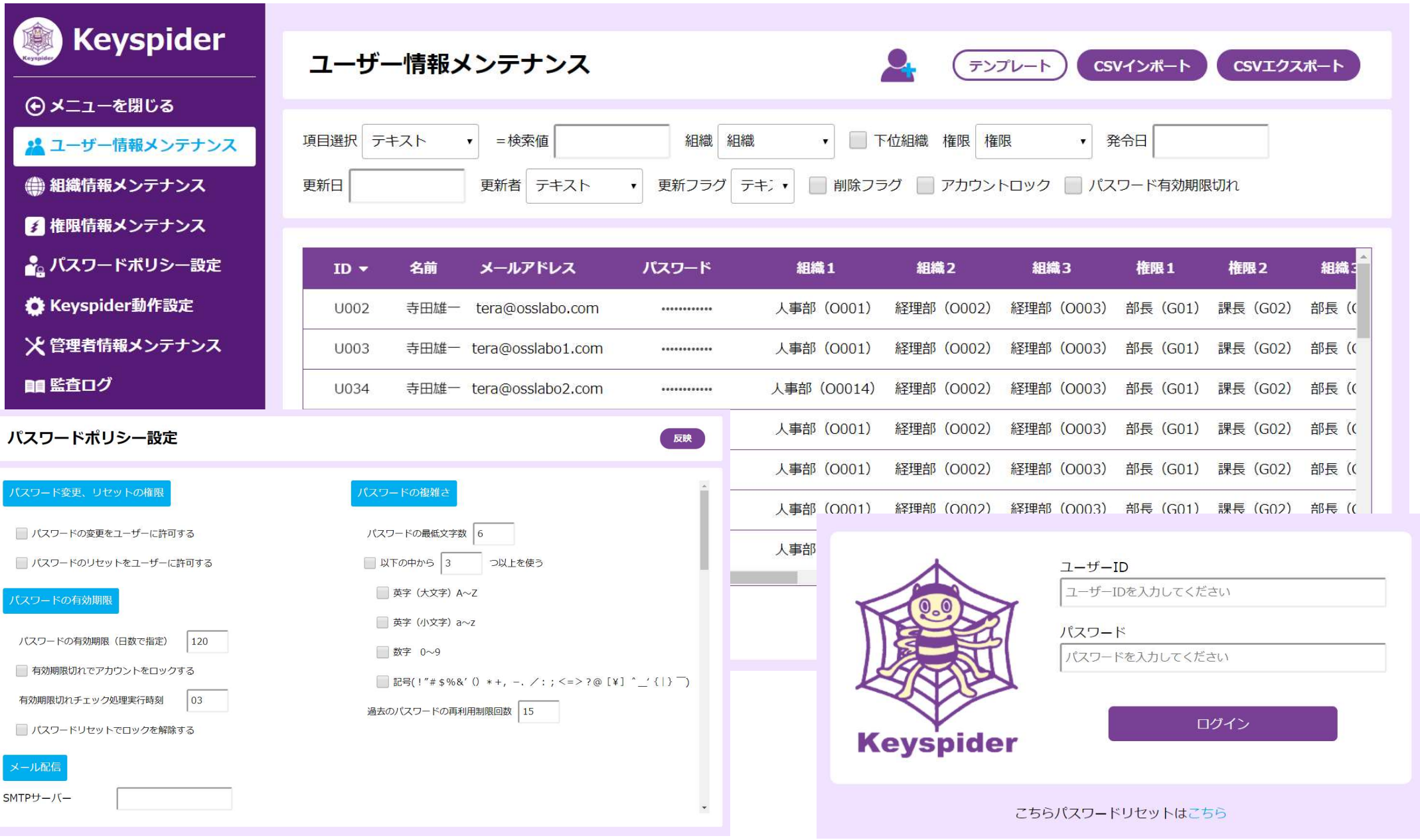
独自のセキュア通信機能で、オンプレとも安全に連携



ユースケース

源泉		連携先システム
Oracle/AD /CSV 他にもLDAPなど 複数の源泉があるパターンも	Keyspider	社内システム / AD/AzureAD 各種クラウドサービス
AzureAD 他にもIDaaSなど	Keyspider	社内システム / AD/AzureAD 各種クラウドサービス
Keyspiderが 源泉となるパターン	Keyspider	社内システム / AD/AzureAD 各種クラウドサービス

KeyspiderManager



Keyspiderの主な機能

機能名	内容
データ取込	人事ステム（RDB）やAD、CSVファイルからのデータ取込
プロビジョニング（データ同期）	社内システムやクラウドサービスなどへのデータ同期
属性編集・マッピング	データ同期時に連携する相手システムの項目に合わせて柔軟に項目を編集、マッピング
社員番号、メールアドレスなどの生成（関数機能）	ルールに基づき、自動的に社員番号やメールアドレスを生成
発令日前後の日程でデータ同期	例えば入館証作成のために、発令日前にプロビジョニングをする必要があるケースへの対応（オプション）
異動後一定期間、旧権限を保持	例えば異動後2週間は、異動前の権限も使えるようにする（オプション）
有効期限によるアカウント削除、権限削除（予定）	予め有効期限（例えば6か月など）を決めて、アカウントを登録したり権限を付与する（期限後に自動的に削除される）
新規アカウント登録時の自動権限付与（予定）	新規アカウント登録時に、予め指定されたポリシーに従って自動的に権限を付与

Keyspiderの主な機能

機能名	内容
マスタ管理	各システムのユーザー、組織、権限の一元管理 管理者やヘルプデスクによる、データの検索とメンテナンス CSVインポート
パスワード管理	パスワードポリシー設定 有効期限切れリマインドメール ユーザー自身による、パスワード変更とパスワードリセット
承認ワークフロー（予定）	アカウント登録や権限付与について、マネージャー等の承認を経てから実行する
差分チェック（予定）	KeyspiderのDBと、プロビジョニング先の状態に差分が無いかをチェック
異常値アラート（予定）	プロビジョニング用のデータ作成時、通常とは異なる大量の差分が発生した場合などに警告
棚卸データ作成（予定）	システム上のアカウントや権限の状態と実際の現場との乖離をチェックする棚卸業務のために必要なデータを生成
監査証跡	Keyspider Manager（画面）において、いつ、誰が、どのような操作を行ったのかのデータを記録

料金

	マネージドサービス	ソフトウェア提供（サブスクリプション型）	ソフトウェア提供（ライセンス販売型）	オープンソース
Keyspider Core（ID連携機能）	○	○	○	○
KeyspiderManager（管理画面）	○	○	○	×
マネージドサービス	○	×	×	×
サポート	○	○	○	×
料金体系	**月額利用料（サブスクリプション型）**	月額利用料（サブスクリプション型）	ライセンス販売＋年間保守費用	—
料金	お問い合わせください	お問い合わせください	お問い合わせください	無料
備考	初期費用：30万 連携設定作業代行：20万～/システム			

■各システムとの連携

連携状況（続々検証中）

No.	名称	種別	方向	方式	状況・備考
01	CSVファイル	オンプレ	入力・出力	CSV	○
02	AD/LDAP	オンプレ	入力・出力	LDAP	○
03	RDB/Oracle	オンプレ	入力・出力	SQL	○
04	AzureAD	クラウド	入力	SCIM	○
05	AzureAD/Microsoft365	クラウド	出力	GraphAPI	○
06	GoogleWorks	クラウド	入力・出力	SCIM	検証中
07	Okta	クラウド	入力・出力	SCIM	検証予定
08	OneLogin	クラウド	入力・出力	SCIM	検証予定
09	トラスト・ログイン	クラウド	出力	SCIM	○
10	IIJ ID	クラウド	入力・出力	SCIM	検証予定
11	Slack	クラウド	出力	SCIM	○
12	Zoom	クラウド	出力	SCIM	○
13	BOX	クラウド	出力	SCIM	○
14	Salesforce	クラウド	出力	SCIM	○
15	SAP	クラウド	出力	SCIM	検証予定
16	コンカー	クラウド	出力	SCIM	検証予定
17	奉行クラウド	クラウド	出力	RPA	○
18	ジョブカン	クラウド	出力	RPA	○
19	SmartHR	クラウド	出力	RPA	○
20	楽々清算	クラウド	出力	RPA	○
21	（続々検証中）				

ぜひ、こちらもご覧ください

KAMOME Engineering

ご紹介動画も公開中です。

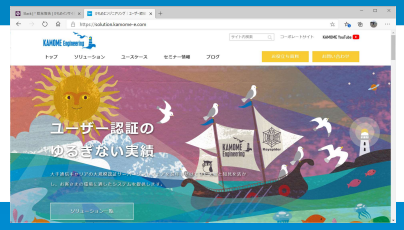
YouTube
「Keyspider」
で検索

YouTube「KAMOME Channel」

シングルサインオンのご紹介や、過去セミナー動画などもあります。

ありがとうございました

当社プロダクトに関係するテーマで
Webセミナーを開催しています。（月2～3回程度）
さまざまな立場の方にご参加いただいております。



ソリューションサイト、リニューアルしました。
https://solution.kamome-e.com/

オライリー・ジャパン社より出版。
当社 および 当社メンバーが、執筆・翻訳に携わりました。

お問い合わせはコチラから ➡➡

または　✉ i-sales@kamome-e.com

かもめエンジニアリング株式会社

KAMOME Engineering
日本でいちばん仕事が大好きなチームです！